

U.S. Department of Justice

Federal Bureau of Investigation



Washington, D.C. 20535-0001

FOR IMMEDIATE RELEASE

NATIONAL PRESS OFFICE

December 19, 2014 [\(202\) 324-3691](tel:2023243691)

www.fbi.gov

Update on Sony Investigation

Today, the FBI would like to provide an update on the status of our investigation into the cyber attack targeting Sony Pictures Entertainment (SPE). In late November, SPE confirmed that it was the victim of a cyber attack that destroyed systems and stole large quantities of personal and commercial data. A group calling itself the “Guardians of Peace” claimed responsibility for the attack and subsequently issued threats against SPE, its employees, and theaters that distribute its movies.

The FBI has determined that the intrusion into SPE’s network consisted of the deployment of destructive malware and the theft of proprietary information as well as employees’ personally identifiable information and confidential communications. The attacks also rendered thousands of SPE’s computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company’s business operations.

After discovering the intrusion into its network, SPE requested the FBI’s assistance. Since then, the FBI has been working closely with the company throughout the investigation. Sony has been a great partner in the investigation, and continues to work closely with the FBI. Sony reported this incident within hours, which is what the FBI hopes all companies will do when facing a cyber attack.

Sony’s quick reporting facilitated the investigators’ ability to do their jobs, and ultimately to identify the source of these attacks.

As a result of our investigation, and in close collaboration with other U.S. Government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions. While the need to protect sensitive sources and methods precludes us from sharing all of this information, our conclusion is based, in part, on the following:

Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks.

The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. Government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known

North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack.

Separately, the tools used in the SPE attack have similarities to a cyber attack in March of last year against South Korean banks and media outlets, which was carried out by North Korea.

We are deeply concerned about the destructive nature of this attack on a private sector entity and the ordinary citizens who worked there. Further, North Korea's attack on SPE reaffirms that cyber threats pose one of the gravest national security dangers to the United States. Though the FBI has seen a wide variety and increasing number of cyber intrusions, the destructive nature of this attack, coupled with its coercive nature, sets it apart. North Korea's actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves. Such acts of intimidation fall outside the bounds of acceptable state behavior. The FBI takes seriously any attempt – whether through cyber-enabled means, threats of violence, or otherwise – to undermine the economic and social prosperity of our citizens.

The FBI stands ready to assist any U.S. company that is the victim of a destructive cyber attack or breach of confidential business information. Further, the FBI will continue to work closely with multiple departments and agencies as well as with domestic, foreign, and private sector partners who have played a critical role in our ability to trace this and other cyber threats to their source. Working together, the FBI will identify, pursue, and impose costs and consequences on individuals, groups, or nation states who use cyber means to threaten the United States or U.S. interests.